[19] 中华人民共和国国家知识产权局

[51] Int. Cl⁷
H04L 12/54
H04L 29/06

[12] 发明专利申请公开说明书

[21] 申请号 01139210.X

[43] 公开日 2003 年 7 月 9 日

[11] 公开号 CN 1428980A

[22] 申请日 2001.12.26 [21] 申请号 01139210.X

[71] 申请人 上海贝尔有限公司
地址 201206 上海市浦东新区金桥出口加工区宁桥路 388 号
[72] 发明人 陆学峰

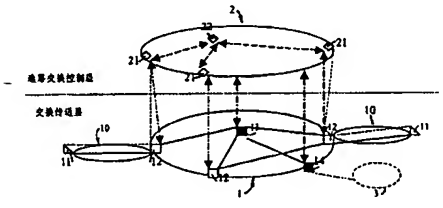
[74] 专利代理机构 上海专利商标事务所
代理人 章蔚强

权利要求书 1 页 说明书 15 页 附图 2 页

[54] 发明名称 一种基于带外信令的 IP 网络系统

[57] 摘要

一种基于带外信令的 IP 网络系统，它由端到端的 MPLS 交换传送层和控制这一交换传送层的选路交换控制层组成，其中：MPLS 交换传送层由若干边缘的 MPLS 交换机和一些中转的 MPLS 交换机在传输链路连接下构成，并通过接入网连接至用户；选路交换控制层由一或若干个选路交换控制器和信令链路网构成，在上述的网络中，还包含两类控制器：一系列边缘的选路交换控制器和连接它们的若干个中转的选路交换控制器。 本发明保证了常人对网络公共设施的不可接入性，提供“通信用户识别和捣乱用户追查处理”等安全功能，从而提供了电信级的网络安全性。 另外不仅如此，还进一步提高了网络的传送效率，更好地保证了电信级的服务质量，并同时解决了现行因特网协议版本 4 (IPv4) 地址空间不足的问题。



ISSN1008-4274

1．一种基于带外信令的 IP 网络系统，其特征在于，它由端到端的 MPLS 交换传送层和控制这一交换传送层的选路交换控制层组成，其中：MPLS 交换传送层由若干边缘的 MPLS 交换机（12）和一些中转的 MPLS 交换机（13）在传输链路连接下构成，并通过接入网（10）连接至用户（11）；选路交换控制层由一或若干个选路交换控制器（21/22）和信令链路网构成，

在上述的选路交换控制层中，有两类控制器：一系列边缘的选路交换控制器（21）和连接它们的若干个中转的选路交换控制器（22），选路交换控制器对其所管豁的 MPLS 交换机进行控制，包括建立与更新 MPLS 交换机的标签路由表；同时为通信的会晤或呼叫选择适当的标签交换路径和进行会晤/呼叫过程的控制，所有的选路交换控制器都是由带有通信接口的处理器平台再加上软件控制器所组成；

上述的选路交换控制器之间，选路交换控制器与其所管豁的 MPLS 交换机之间都将由专门的信令链路进行连接与通信，用户与网络也将通过信令来交换服务请求与服务控制的信息，在物理上上述的信令链路可以由多种传送媒体构成，也可以通过 MPLS 交换传送网本身来传送，在此系统下，用户数据不再进行 IP 层的包装，将直接装入 MPLS 帧中进行传递。

2．根据权利要求 1 所述的一种基于带外信令的 IP 网络系统，其特征在于，在所述的选路交换控制层中进行路由的选择，网络寻址与服务信息的信令传送与交换，并对所豁的 MPLS 交换机进行控制，建立要求的标签交换路径。

3．根据权利要求 1 所述的一种基于带外信令的 IP 网络系统，其特征在于，在所述的网络结构系统中的接入网（10）必须是点到点或点到多点的结构，以便边缘的 MPLS 交换机（12）可以从物理上对用户进行定位。

4．根据权利要求 1 所述的一种基于带外信令的 IP 网络系统，其特征在于，所述的选路交换控制层具有网络安全服务功能，可由信令向远程终端提供信息发送者或呼叫主叫的识别功能。

一种基于带外信令的IP网络系统

(一)技术领域

本发明涉及通信信息技术领域中一种基于带外信令的 IP（因特网协议）网络架构。

(二)背景技术

众所周之，传统的 IP 网络（目前的因特网），是依靠路由器及其所运行的路由协议进行IP数据包的转发的（参看图1a)。由于其良好的互连性能和经济简易，使得它得到了超常规的发展和广泛的应用。从网络结构的角度上看，常见的有：传统的由一系列IP路由器组成的采用全选路方式的网络架构（如图 1a 所示)、采用MPLS（多协议标记交换）协议的由若干中继MPLS交换机62和IP边缘选路交换机61组成的较新的IP网络架构（如图1b所示），这些网络架构存在着三大问题，一直困扰着电信信息业界。其一是服务质量（QoS）问题；二是网络安全问题；三是当前的因特网协议版本IPv4（因特网协议版本4）地址空间不足。

目前的电信级IP网络主要是针对QoS的，即希望能建立一个具有电信级服务质量的 IP（因特网协议）网络。为此一系列新的协议已经应运而生，如综合服务协议（intserv）(RFC 1633)，差别服务协议（diffserv）(RFC 2475)，资源预留协议（RSVP）(RFC 2205)等。与此同时这里还要特别提到MPLS（其框架协议为RFC 3031 ）这一重要的协议。MPLS并不是专为解决QoS而提出的。MPLS首先是要大大减少IP数据包选路转发的次数，将选路转为高效的标记交换，从而提高IP数据包传送的效率与速度。但同时它也为QoS的定量保证以及IP的网络工程提供了良好的解决办法。如果再采用多协议标记交换论坛（MPLS Forum）建议的，并得到世界电信联盟电信标准部(ITU-T)支持的将语声载于多协议标记交换(Voice over MPLS 或 VoMPLS)。它还将为IP网络传送实时信号（如语声等）提供良好的解决办法。

但是作为电信级的IP网络仅仅解决QoS是不够的，还必须具有电信级的安全。

目前对于电信级 IP 网虽然还没有提高到电信级网络安全这一高度。但不少电信信息专家都在为网络的安全进行工作和研究。但他们绝大部分的工作是集中在加密系统的研究（包括各种新的加密算法）、认证与授权的方法，信息完整性的检测，不可拒绝性的证明等，以及如何将它们使用到通信协议之中，作为产品则有防火墙，安全网关，抗病毒软件等等。可以在大量的文献书籍中看到上述各方面的工作。也有人在软件体系的研究中，建议将认证与加密功能，以及对异常使用的监察功能等做到中间件中（例如 TINAC（通信信息连网架构联合会））。但仅仅靠这些手段是不够的，而且这些手段需要很多的处理能力，大大提高了系统的复杂程度。

IP（因特网协议）网络在安全上一个致命的弱点是采用了带内信令的网络机制，即信令（控制信息）和用户数据是装在一个数据包中传送的，（参看图 1a), 1b)）。按照因特网协议（RFC 791），IP 数据包是由控制包头和要传送的用户数据在一起构成的。包头中有协议版本、源地址、目的地地址、服务类型、生命长度等等都是网络选路与处理所需要的控制信息。按电信的说法，这是一种带内的信令信息。也有的 IP 包，如 ICMP（因特网控制消息协议）协议数据包，是专用于传送控制信息的。但它处于 IP 层的上层，具有普通 IP 数据包同样的信头，须在到达目的地路由器后，先将它打开才能取出其中的路由更新等信息。总之按照这一协议用户数据与控制信息走的是同一路由。路由器按包头进行选路，不管这 IP 包是传送用户数据的，还是网络控制信息的。这种带内的信令机制给网络的公共设施，如路由器、交换机等在安全上带来了如下的脆弱性：

1) 由于控制信息与用户数据是在一起的，走在同样的路由上。一般的用户（非网络管理员）只要知道公共设施的 IP 地址，并能通过口令、密钥等各种认证和解密关，就可以像接入终端主机一样接入到网络的公共设施，因而可能对公共的路由器或交换机进行控制、修改、监视和破坏。

2) 用户的 IP（因特网协议）数据包包括有发送者地址，接收人地址和用户信息内容在内的完整的用户信息，这使信息在窃听时很容易被完整地窃取，并容易对它进行跟踪和破坏。

除了网络公共设施的安全外，还有端到端的通信安全问题。即黑客/窃客非法接入或破坏它无权接入的主机、数据中心、网站、数据库、LAN（局域网）和应

用服务器等。这些数据终端的安全主要也是靠接入的检查、认证和加密等措施来保护的。但目前广泛采用的口令式的认证常被证明是不可靠的。口令（password）很容易被窃取和用穷举等算法所破译，从而导致终端、网站被黑，服务器拒绝服务，软硬件被破坏，数据被删改等。

上述网络公共设施的安全和用户端到端的通信安全问题都有待在网络结构上提供解决办法。

因特网地址空间不足的问题也是与采用带内的信令方式直接相关的。目前建议的解决办法是采用 IPv6(因特网协议版本 6)，将地址长度扩展到 128 位。但这一解决办法存在着如下缺点：

a)由于 IPv4（因特网协议版本 4）在服务质量和安全方面的改进，IPv6(因特网协议版本 6)除了地址空间上的优势外，已经没有其它特别的优点。但它确会带来一系列协议的修改。

b)由于协议的不同，IPv4 的网络与 IPv6 网络将成为两个不同的网络，需要通过双协议栈或隧道连接等方法解决互连互通问题。网络从目前的 IPv4 过渡到全 IPv6 将是一个长期而痛苦的过程。

c)IPv6 由于地址长，开销将更大，路由器的实现也将更加困难，或者说需要更高的技术或成本。

但若采用本发明建议的带外信令方式，地址空间的问题将很容易解决。

(三)发明内容

基于 IP（因特网协议）网络发展中的先进技术，特别是 MPLS 协议的技术优势，针对现有 IP 网络在安全方面的问题和地址空间问题，本发明提出一种改进的 IP 网络系统，目的是使该 IP 网络系统不仅在服务质量（QoS）上，而且在网络安全上都达到电信级的要求，并同时解决地址空间问题。

本发明所提供的一种基于带外信令的 IP 网络系统，它由端到端的 MPLS 交换传送层和控制这一交换传送层的选路交换控制层组成，其中：MPLS 交换传送层由若干边缘的 MPLS 交换机（12）和一些中转的 MPLS 交换机（13）在传输链路连接下构成，并通过接入网（10）连接至用户（11）；选路交换控制层由一或若干个选路交换控制器（21/22）和信令链路网构成，在上述的选路交换控制层中，可能

有两类控制器：一系列边缘的选路交换控制器（21）和连接它们的若干个中转的选路交换控制器（22），选路交换控制器对其所管辖的 MPLS 交换机进行控制，包括建立与更新 MPLS 交换机的标签路由表；同时为通信的会晤或呼叫选择适当的标签交换路径和进行会晤/呼叫过程的控制，所有的选路交换控制器都是由带有通信接口的处理器平台再加上软件控制器所组成；上述的选路交换控制器之间，选路交换控制器与其所管辖的 MPLS 交换机之间都将由专门的信令链路进行连接与通信，用户与网络也将通过信令来交换服务请求与服务控制的信息，在物理上上述的信令链路可以由多种传送媒体构成，也可以通过 MPLS 交换传送网本身来传送，在此系统下，用户数据不再进行 IP 层的包装，将直接装入 MPLS 帧中进行传递：

上述的基于带外信令的 IP 网络系统，其中，在所述的选路交换控制层中进行路由的选择，网络寻址与服务信息的信令传送与交换，并对所辖的 MPLS 交换机进行控制，建立要求的标签交换路径。

上述的基于带外信令的 IP 网络系统，其中，在所述的网络结构系统中的接入网（10）必须是点到点或点到多点的结构，以便边缘的 MPLS 交换机（12）可以从物理上对用户进行定位。

上述的基于带外信令的 IP 网络系统，其中，选路交换控制层具有网络安全功能，由信令向远程终端提供信息发送者或呼叫主叫的识别功能。

采用上述方案：(1) 由于采用带外的信令方式，网络公共设施中的各选路交换控制器和各 MPLS 交换机都是经由专门的信令来进行控制与通信的。用户与网络只能经由用户网络信令传递服务请求和对服务的控制进行响应，并经由数据通信信道传送用户数据。这一结构保证了一般用户对于网络公共设施管理与控制的不可接入性。此外在本结构下，网络可以通过对用户物理线位/端口的识别来进行用户的接入控制/认证；并可向远程的终端（含各种终端、应用服务器、数据库、网站等）提供发送者/主叫用户的识别与认证。以上两点将使这新 IP 网络具备电信级的网络安全性。(2) 也由于采用带外信令，在用户平面，也即在交换传送层中，不再有三层（即 IP 层）的处理，MPLS 数据包中也不必再有三层的控制信息，可以大大减少传输的开销，提高网络传送的效率与速度。从而进一步提高网络的服务质量（QoS）。(3) 还是由于采用带外信令，网络地址（包括源地址、目的地地址和转送

地址等）将只是信令中的一个参数。不需要因为地址空间不足而修改网络协议。地址的长度将可按需而定，并且是可以改变的。这将彻底解决网址不足的问题。

(四)附图说明

图 1a 是现有的全 IP 选路（routing）的 IP 网络；

图 1b 是现有基于 MPLS 的 IP 网络；

图 2 是本发明基于 MPLS 和分层的 IP 网络系统；

图 3 是本系统中无连接服务流程的示意图；

图 4 是本系统中面向连接服务流程的示意图。

(五)具体实施方式

本发明提出了将现有 IP（因特网协议）传送网分为两层来实现的网络结构，它由端到端的 MPLS（多协议标签交换）交换传送层和控制这一交换传送层的选路交换控制层组成（参看图 2）。其中 MPLS 交换传送层由若干边缘的 MPLS 交换机 12 和一些中转的 MPLS 交换机 13 在传输链路连接下构成，并通过接入网 10 连接至用户 11。选路交换控制层由一或若干个选路交换控制器 21/22 和信令链路网构成，在一个较大的网络中，将包含两类控制器：一系列边缘的选路交换控制器 21 和连接它们的若干个中转的选路交换控制器 22。选路交换控制器对其所豁的 MPLS 交换机进行控制，包括建立与更新 MPLS 交换机的标签交换路由表；同时为通信的会晤（session）或呼叫选择适当的标签交换路径和进行会晤/呼叫过程的控制。所有的选路交换控制器都是由带有通信接口的处理器平台再加上软件控制器所组成。有关各种 MPLS 交换机和选路交换控制器的功能及它们间的相互作用将在后面作具体的定义。上述的选路交换控制器之间，选路交换控制器与其所管豁的 MPLS 交换机之间都将由专门的信令链路进行连接与通信。用户与网络也将通过信令来交换服务请求与服务控制的信息（用户网络信令）。在物理上上述的信令链路可以由多种传送媒体构成，也可以通过 MPLS 交换传送网本身来传送。在此系统下，用户数据不再进行 IP 层的包装，将直接装入 MPLS 帧中进行传递。以下子特征对于本系统是重要的：

1）.网络的寻址信息将经由信令在选路交换控制层中进行传送与交换。信令中地址字段的长度可以是固定的，也可以是不固定的。在不固定时须在地址字段中增

设一个地址长度子字段。因而地址长度可以与 IPv4(因特网协议版本 4)相同，也可与 IPV6（因特网协议版本 6）相同，还可以与两者都不同。与此同时还可以采用有等级架构的长度可变的地址方案及相应的寻址方式。

2）.本发明的网络结构将原先计划用于核心网 6（参看图 1b)）的 MPLS（多协议标签交换）技术扩展到了用户终端/用户网络（参看图 2)。在接入网区段 10，标签被用来区分信令、维护控制信息与用户数据，也用于用户 11 的识别。后面会对 MPLS 在接入网上的扩展进行具体的定义。

3）.本发明的网络结构还规定公众的接入网 10 必须是点到点或点到多点的结构，以便边缘的 MPLS 交换机可以从物理上对用户 11 进行定位。这种定位将作为对用户进行入网控制的重要手段之一。

4）.作为选路交换控制层在网络安全上的必备功能，它必须能经由信令向远程终端（含一般主机、应用服务器、数据库和网站等）提供信息发送者或呼叫主叫的识别功能（包括与它们物理定位相对应的识别信息及其它信息)。作为远程接入控制的重要手段之一。

本发明提出了一种将选路交换的控制与交换传送（即数据包转发（forwarding））相分离（分层）的，采用带外信令的网络架构（图 2)。这一架构的交换传送层将采用端到端 MPLS 的传送协议。即 MPLS 将不仅用于核心网 1，也将用于接入网 10。新架构的控制层将由集中或分散的一系列控制服务器 21/22 组成。控制层的各服务器之间，控制层与终端之间以及控制层与 MPLS 交换机之间将采用适当的信令进行通信，以完成对网络与服务的控制。网络的架构可以用图 2 加以示意。

（1）MPLS（多协议标签交换）交换传送层

交换传送层由用户终端/用户网 11、接入网 10、核心网 1 三部分构成（参看图 2)。

用户终端/用户网 11 的功能是向用户提供各种应用，可以联网工作和非联网工作。直接联网工作的终端或用户网网关必须有网络通信功能，其二层是基于现有的二层（如以太网（Ethernet），异步传送方式（ATM）,帧中继（FR）等）或新的二层协议并加了标签后形成的 MPLS 层。物理层可以是多样的，由接入网决定。终

端的高层由所需的应用而定。但在本架构中三层的信令是不可少的。用户数据将经由 MPLS 层包装后直接送入网络。用户终端可以直接与接入网相连，也可以经由用户网的网关与外部网络相联。用户网是用户在户内进行通信的网络，可以是局域网（LAN）、户内电话线连网（HomePNA）、电力线连网（PowerLine）、无线局域网（WLAN）及兰牙等种种网络。

接入网 10 最基本的功能是用户的汇聚，即将大量的用户经复用、汇合后经较少的线路端口接入到一或多个本地的 MPLS 交换机上。接入网的物理层可以多种多样，包括现有的各类数字用户环路（xDSL），电缆调制解调器（CableModem），以太网无源光网络（EPONz）或 ATM 无源光网络（APON）疏波分复用（CWDM）和各种宽带无线接入系统等。但其二层与终端一样，是基于现有二层（如 Ethernet, ATM, FR 等）或新的二层协议并加了标签后的 MPLS 层。最基本的接入网除了须用 MPLS 信道传送用户网络信令和经 MPLS 包装的用户数据外，可以不需要三层以上的协议和应用。但在特定情况下，基于因特网接入提供商/因特网服务提供商（IAP/ISPs）提供特定服务的需要，也可能加入三层以上的功能，甚至还可能有本地的应用服务器。

核心网 1 由一系列 MPLS 交换机在传输链路的连接下组成，完成端到端的数据交换与传送。MPLS 交换机的功能是依据数据包上所打的标签转发（forwarding）数据包。按照所担负的功能可分为边缘的 MPLS 交换机 21、中继的 MPLS 交换机 22（在一个小的网络中，这两者也可能合二为一，即只有一个 MPLS 交换机）。边缘 MPLS 交换机 21 的工作是汇集用户接入网 10 的用户网络信令并馈送给相应的控制服务器，同时汇集其用户接入网 10 的用户数据流，根据在选路交换控制层控制下建立与更新的标签交换路由表，将用户数据发送到指定的出口，连往另一个 MPLS 交换机；或将外来的用户数据按标签送达终端用户 11。中继的 MPLS 交换机 13 负责 MPLS 数据帧的中转。它们同样在选路交换控制器控制下建立与更新标签路由表。按输入数据帧的标签，按要求更换标签，并送达相应的出口。一般地说 MPLS 交换机是低智能的，除了必要的本地维护管理功能，差错检测与报告功能以及信令功能等以外，都是在控制层服务器的控制下进行正常工作的。

（2）选路交换控制层

选路交换控制层由一系列用于选路交换的控制器21/22（或称控制服务器）和信令链路网构成。依据网络的规模和不同的实现方案，选路交换控制层可以是集中的，或分散的。如果网络不很大，服务器的处理能力又足够，可以用一个集中的控制器（或者为了可靠可以再设一个备份控制器，或采用双机均分负荷的工作方式），来控制整个网络。也可以是分散的。在一个容量很大的网络中，可以由一系列边缘控制器21，每一个与一或多个边缘的MPLS交换机12相对应，负责一个本地区域的服务。为了沟通这些边缘控制器，可能还需要有一些中转的控制器22，并可以利用这些中转的控制器22对中转的MPLS交换机13进行控制或转发控制器到控制器的信令。选路交换控制器之间，选路交换控制器与所豁的MPLS交换机之间将经由信令链路连接起来，以实现通信和对MPLS交换机的控制。边缘的选路交换控制器21还经由用户网络信令与直接连网或经接入网10连网的用户终端或用户网网关11进行通信，传递用户的通信会晤/呼叫等服务的请求，并对服务过程进行控制。

选路交换控制层的基本功能如下：

a)依据用户的注册，为每一个用户建立服务文档（即service profile）。

b)在用户请求通信时先与用户交换用户网络信令，依据用户网络信令提出的服务请求和对用户服务文档的查询，来启动数据包的路径选择（在提供无连接服务时（connectionless service））和/或呼叫连接的建立功能。如果所需的标签交换路径（LSP）已经存在，只需要通过信令为用户数据包赋于适当的路由标签。如果无适当的LSP，就需按照下面c)点建立新的LSP。然后再将标签用信令通知用户。

c)依据适当的选路算法，并通过与相关控制器和与MPLS交换机之间的信令交换，为用户数据包建立符合用户服务要求的，也就是能通达各要求目的地，又符合一定服务质量要求的MPLS的标签交换路径；并确定与保持这标签交换路径的可用性。

d)依据选定的标签交换路径对MPLS交换机进行控制（即建立与更新标签路由表），在物理上实现这些标签交换路径。

e)对于用户面向连接的服务，选路与交换控制层还要有连接的建立、保持与释放功能。

f)控制层在需要时还可与应用服务器进行通信，来提供补充服务或增值服务。

g)控制层本身可以有管理功能，也可与外部的管理服务器进行通信，来进行计费与网络的管理等。

出于安全的角度，选路交换控制层还可以有如下的安全服务功能：

a)在边缘 MPLS 交换机的配合下，完成入网用户的识别和捣乱用户的追查功能。并能向远程终端（含应用服务器、数据库或网站等）提供信息发送者/主叫用户的识别，供认证时使用。这一点在后面还将详细介绍。

b)必要时可建立用户通信信用数据库，供被叫终端（含应用服务器、数据库或网站等）在认证用户的接入时进行查询。

c)在信令链路需要经由外部网络传送时，须要进行链路两端间的认证和信令信息的加密处理。

d)其它可能需要的安全措施。

下面介绍上述网络架构中的各主要功能实体。这此功能实体可以单独构成设备，也可以多个功能实体，包括不同的功能实体放在一起来构筑设备。本架构涉及的只是数据包的二、三层传送与处理的功能实体。包括 MPLS 交换机（包括边缘的 12 和中转的 13）。选路交换控制器（包括边缘的 21 和中转的 22）。还有互通单元 14。这是与现有 IP 网络或其它网络 3 互通所必须的。

(1) MPLS 交换机 12/13

在本网络架构下，MPLS 交换机是处于交换传送层的一个低智能的交换实体，它的基本功能如下：

a)能与一或多个选路交换控制器交换信令，并依据控制器的指令建立与更新标签选路表。根据这一标签路由表，交换机能依据入局数据包的标签将数据包送往指定的路由出口。并为这入局的数据包更换标签，以便下一局站的选路。

b)能自动监控自身的资源状况，包括端口的数量与状态，各路由的带宽，交换机处理能力和各路由带宽的使用状况。并能将这些状况，特别是各种资源的可用性通过信令报告给相关的控制器。或接受控制器的询问。

c)可以就地对交换机的资源进行分区（partitioning）与指配，也能远程地接受控制器的命令，对交换机的资源进行分区与指配。当存在着多个控制器时，将只允

许一个控制器（主控器）对整个交换机进行分区与指配工作。但其它控制器在其各自负责的分区内，也可有资源的控制（甚至再分区）与指配能力。

d)交换机的分区功能，将使一个物理的交换机可以为多个 ISPs 共享。

作为 MPLS 的边缘交换机 12，它还应该具有边缘交换机如下特有的功能：

a)在物理上识别接入的用户 11。

b)对用户发出的信令进行初步的检查(即判明这是一条符合规格的用户网络信令）后，转发给选路交换控制器。和将控制器的用户网络信令转发给用户。

c)在控制器或操作人员的控制下对用户与接入网进行维护检查。

(2)选路交换控制器 21/22

选路交换控制器具有类似于路由器中控制部分的功能。在本网络架构下，它是处于选路交换控制层中的高智能的控制实体，是由带有通信接口的处理器平台再加上控制软件组成的。在一个较大的网络中，选路交换控制器可分为两类：一类是具有边缘选路与交换功能的控制器 21。另一类是中转的选路交换控制器 22。

具有边缘选路与交换功能的控制器在功能上较为复杂，其基本功能如下：

a)用户网络信令实体功能。它经由边缘的 MPLS 交换机，经由信令信道与用户交换通信请求、需求和会晤/呼叫的控制信息。

b)用户的服务文档数据库。它寄存用户的服务注册信息和识别信息。

c)通信会晤/呼叫的处理功能。依据用户信令送来的服务请求和用户的服务文档进行通信会晤（session）/呼叫(call)的处理。

d)选路功能。选路交换控制器具有路由表。这路由表可以是人工静态地配置的；也可以是通过与其它控制器交换信息，确立网络的拓朴结构，并依据一定的路由算法自动地生成的。选路功能依据目的地地址和服务质量等要求等创建等效的转发类别（FECs）(参看 RFC 3031)，并由路由表将不同的 FEC 映射为不同的标签交换路径（LSP）和相应的标签堆栈（Label stack），并将它传送给连网的用户终端或用户网网关。

e)控制器到控制器信令功能。用于与其它控制器交换信息，以完成选路功能和会晤/连接的控制功能。

f)控制器到 MPLS 交换机的信令功能。用于对相应的边缘的 MPLS 交换机，

和所管辖的中转的 MPLS 交换机进行控制，建立与更新标签路由表。

g)维护、管理和计费等功能（可能是内置的，也可能是外置的）。这一功能完成用户接入部分，控制器实体本身以及边缘的 MPLS 交换机的资源管理和维护管理功能，以及通信的计费功能等。这管理功能中可能包括对一个物理的 MPLS 交换设备进行资源配置和分区配置，甚至包括对各分区以内的资源配置和子分区管理。

中转的选路交换控制器功能 22 较为简单，可能的功能如下：

a)控制器到控制器信令功能。用于与其它控制器，特别是边缘的选路交换控制器交换信令信息，以完成选路功能和会晤/连接的控制功能。

b)信令的汇聚与转接功能（类似于七号信令的 STP）。

c)对所管辖的中转的 MPLS 交换机 13 进行控制。

d)维护管理功能，对本控制实体与所辖的中转的 MPLS 交换机进行资源管理与维护管理。

（3）互通单元 14

互通单元是与现有网络或其它网络 3 互通所必须的。其具体功能须依据所连接的网络而定。在与现有 IP 网络互通时，其功能在新系统到原系统方向，是从选路交换控制层中取入网址等控制信息与交换传送层 MPLS 帧中的用户数据一起构成 IPv4（因特网协版本 4）的 IP 包即可送入现有网络。在从现有网络到新系统方向，则是进行相反的操作，即将用户数据直接用 MPLS 层协议进行包装，并将网址等相送的控制信息传送给选路交换控制层。

在核心网中 MPLS 交换机的标签是由控制层的选路交换控制器分配的。除此以外标签的分配与使用方法均可以按互联网工程任务组（IETF）的规范（参看 RFC 3031 等）执行。将 MPLS 延伸至接入网后，须要解决终端、用户网网关，甚至接入网小区专用交换机的标签分配问题，以及标签的功能定义问题。对此可采用以下原则：

a)如果用户终端 11 是通过接入网 10 信道与网络的边缘交换机 12 直接相连的。这一终端收发的 MPLS 帧必须符合下面所述的公网要求。

b)如果存在着用户网，用户网内是否采用标签交换，以及标签的使用方法是与

公网无关的。但用户网应该有一个与公网相接的用户网关（在此等价于 11）。这一用户网关的 MPLS 标签应该遵循下面所述的公网要求。

c)如果接入网内存在有接入网交换机，则这一交换机应该有一个与公网相接的用户网络接口（在此也等价于 11）。这一接口上收发的 MPLS 帧应该符合下面所述的公网要求。这一交换机与它服务区内的用户之间是否采用 MPLS，以及其标签的使用方法等也是与公网无关的。

下面即是对上述公网要求的原则性说明：

与核心网 1 一样，标签（Label）的取值只在本地才有意义。接入网 10 的标签，在信息发送一侧，必须有如下功能：

a)区分信令、维护控制信息与用户数据。对于信令和维护信息可以分配固定的标签数值。

b)区分用户数据中不同的服务类别、等级或 QOS。

c)可用于选择想接入的不同的服务提供商（service providers）。

在接收一侧，也即在标签交换路径的末端（如前所述：它可以是用户终端、用户网关或接入网专用交换机的用户网络接口），接入网 10 的标签应具有如下功能：

a)区分信令、维护控制信息与用户数据，对于信令和维护信息可以分配固定的标签数值。

b)区分用户数据中不同的服务类别、等级或 QOS。

c)还可以区分送来数据的不同的服务提供商。

d)MPLS 还将用于识别末端用户 11（包括上述的用户终端、用户网关或接入网专用交换机的用户网络接口等），这种识别末端用户的标签也将由选路交换控制层动态地进行分配，并由信令告知用户。

在这一系统架构中，将涉及到四类信令，用户网络信令，控制器—控制器信令，控制器—交换机信令，以及控制器到应用服务器（包括管理与增值服务等的 AS）之间的信令。这些信令大多可以移用现存的标准信令，在它们的基础上进行修改后得到。开发全新的信令协议也可以，但可能会比较费时。全新的信令系统可以将语声的呼叫处理，多媒体通信的呼叫处理，各种数据会晤的处理以及 IP 包的

Routing 和 Switching 的信令统统都统一起来，并能更好地适应新架构的特点。但基于现有信令修改的办法，不仅开发得快，还可以使原有的软件在修改后继续使用。可以考虑利用或参考的信令有：原电信电信联盟电信标准部（ITU-T）的信令，如：Q.931, Q.2931, Q.761-764(ISUP), Q.BICC（独立于承载的连接控制协议），I.251.3 等，用于数据与多媒体服务的信令，如：H.323, H.248。IETF 的信令：会晤发起协议（SIP），资源予留协议（RSVP），标签分配协议（LDP），还有专门用于控制 MPLS 交换机的通用的交换机管理协议（GSMP）等等。对应该采纳的具体信令的确定不属本专利的范围，这里不想作更多的讨论。但对于选用的信令，在本架构下应该满足如下的要求：

a)应建立一个简练而又统一的信令系统，它将统一用于 IP 包的 Routing, Switching，语声服务的呼叫控制，多媒体服务的会晤处理，各种数据会晤的处理等等。

b)应具有上面所述的通信用户的识别和捣乱用户的追查功能，包括按接入的物理位置，或无线 SIM 卡系统来识别进网的用户，并向远程的终端（包括服务器、网站等）提供发送者识别功能或主叫线识别功能。

c)信令与用户数据不得走同一个标签交换路径（LSP）。信令信息的标签应该是特定的。

d)信令的形式也应采用数据包的方式。

图 3 和图 4 给出了采用本系统提供无连接服务和面向连接的服务的流程的示意图。由于信令是一个有待于其它的专利来规定的系统。在本专利说明中所提供的流程不过是一些概念性的流程，目的是说明整个架构的工作原理。

本架构与原 IP 传送网（包括在核心网中全部采用路由器的和边缘路由器加 MPLS 的（即图 1a)和 1b)），的根本差别是：IP 控制层和交换传送层的全面分离和从带内信令方式改变到带外信令的控制方式；交换传送网将是端到端的 MPLS 网络，即不再用路由器（包括边缘路由器），MPLS 的 LSP（Label Switching Path）将扩展到用户端或用户网络。装于 MPLS 帧中的原 IP 包也不再需要带有原先用于选路（routing）的任何控制信息（包括发送者地址、接收者地址、生命长度（TTL）、服务类型（TOS）等）。

采用上述方案：(1) 由于采用带外的信令方式，网络公共设施中的各选路交换控制器 21/22 和各 MPLS 交换机 12/13 都是经由专门的信令来进行控制与通信的。用户与网络只能经由用户网络信令传递服务请求和对服务的控制进行响应，并经由数据通信信道传送用户数据。这一结构保证了一般用户对于网络公共设施管理与控制的不可接入性。此外在本结构下，网络可以通过对用户物理线位/端口的识别来进行用户的接入控制/认证；并可向远程的终端（含各种终端、应用服务器、数据库、网站等）提供发送者/主叫用户的识别与认证。以上两点将使这新 IP 网络具备电信级的网络安全性。(2) 也由于采用带外信令，在用户平面，也即在交换传送层中，不再有三层（即 IP 层）的处理，MPLS 数据包中也不再有三层的控制信息，可以大大减少传输的开销，提高传送的效率与速度。从而进一步提高网络的服务质量（QoS）。(3) 还是由于采用带外信令，网络地址（包括源地址、目的地地址和转送地址等）将只是信令中的一个参数。不需要因为地址空间不足而修改网络协议。地址的长度将可按需而定，并且是可以改变的。这将彻底解决网址不足的问题。

以上还仅是本系统最为基本的优点。除此以外选路交换控制层还可以提供捣乱用户追查功能，即在网络收到被侵扰的申告时可以立即对捣乱者进行定位，告知被申告人，并将这一捣乱行为记录到这一用户的信用库中。控制层还可以提供捣乱监察功能，对用户发送的数据进行各层次，直到应用层的检查，以发现病毒等有害他方的数据结构。这也将大大加强端到端通信的安全保障。

另外采用分层的网络结构还将带来如下的好处：它使下层的传送技术与上层的控制技术可以分别的发展与更新；可采用一些通用的中间件软件构件（components）来实现对各种交换网络的控制。这些中间件将成为可重用的 COTS（commercial off the shelf）产品。中间件的架构将有开放的接口和 API，因而它的构件（components）可以由许多厂商来共同开发。这将大大提高产品的质量和多样性，从而也导致网络服务的更多样性；在控制能力足够时，一个控制器可以同时管理多个交换机。也可以将一个物理的交换平台进行分区（partition），将其中一些分区租赁给企业或其它运营商，由他们自己的控制器来使用和控制，以构建 VPNs。由于一个物理的交换机可以由多个控制器同时控制。也可能用一个控制器控制多个

交换实体，这将对网络的构建与提供服务将带来新的灵活性。

综上所述，本系统将可提供电信级的安全性；提供比现有电信级 IP 网络更好的服务质量；解决现有 IPv4（因特网协议版本 4）地址空间不足的问题；并可以给设备的组网和服务的提供带来更大的灵活性。

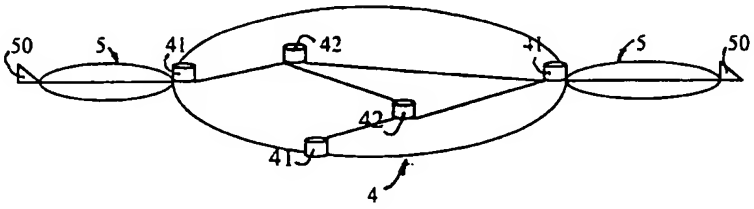

50
5
41
42
41
5
50
42
41
4

图 1a

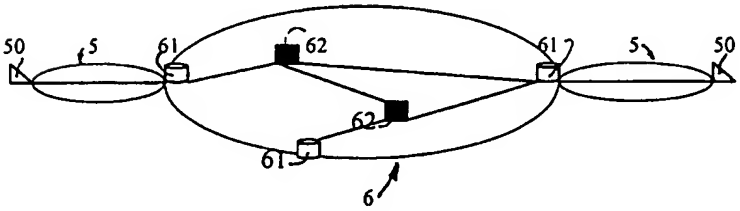

50
5
61
62
61
5
50
62
61
6

图 1b

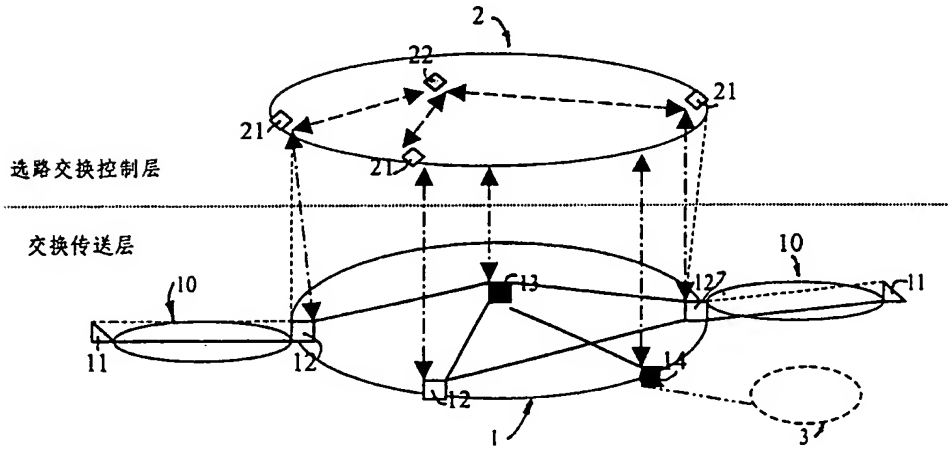

2
22
21
21
21
选路交换控制层
交换传送层
10
10
13
127
11
11
12
12
14
1
3

图 2

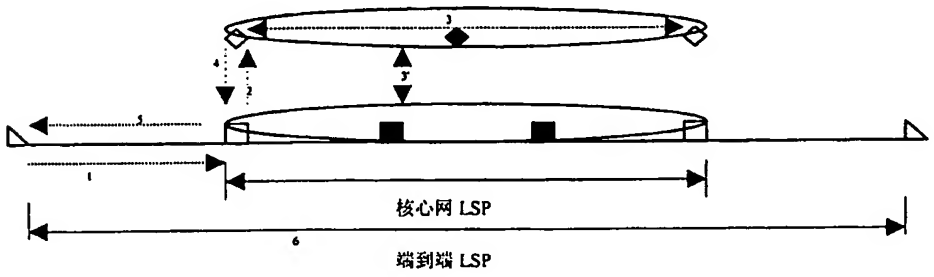


图 3

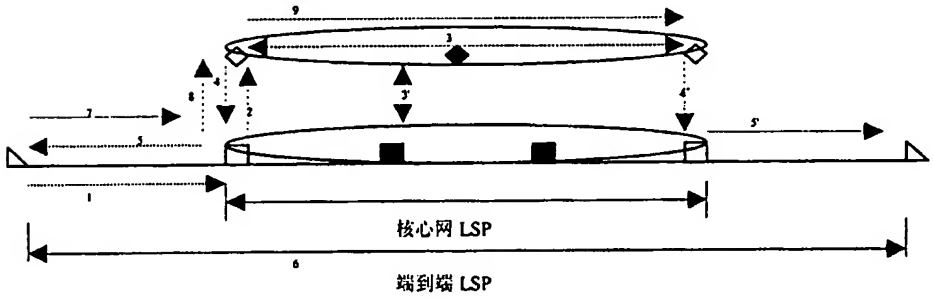


图 4